Nika Aldrich, OSB No. 160306
naldrich@schwabe.com
SCHWABE, WILLIAMSON & WYATT, P.C.
1420 5th Ave., Suite 3400
Seattle, WA 98101
Telephone: (206) 622-1711
Facsimile: (206) 292-0460

Anthony T. Pierce (*pro hac vice*)
apierce@akingump.com
AKIN GUMP STRAUSS HAUER & FELD LLP
2001 K St., N.W.
Washington, D.C. 20006
Telephone: (202) 887-4000
Facsimile: (202) 887-4288

Attorneys for Defendant DarkMatter Group

Clifford S. Davidson, OSB No. 125378
csdavidson@swlaw.com
SNELL & WILMER L.L.P.
601 SW 2nd Ave., Suite 2000
Portland, OR 97204
Telephone: (503) 624-6800
Facsimile: (503) 624-6888

Attorney for Defendants Marc Baier, Ryan Adams, and Daniel Gericke

(Complete list of counsel appears on signature page)

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

LOUJAIN HATHLOUL ALHATHLOUL,

Plaintiff,

v.

DARKMATTER GROUP, **MARC BAIER**, **RYAN ADAMS**, and **DANIEL GERICKE**,

Defendants.

Case No. 3:21-cv-01787-IM

DEFENDANTS' JOINT MOTION FOR CERTIFICATION OF INTERLOCUTORY APPEAL UNDER 28 U.S.C. § 1292(B); MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

LOCAL RULE 7-1 CERTIFICATION

The undersigned counsel hereby certifies that on August 18, 2025, counsel for Defendants discussed the substance of this Motion with counsel for Plaintiff. The parties were unable to resolve the dispute.

MOTION

Defendants DarkMatter Group, Ryan Adams, Marc Baier, and Daniel Gericke hereby move this Court for an order certifying for appeal the Court's July 28, 2025 order granting in part and denying in part Defendants' motions to dismiss, *see* ECF No. 148, pursuant to 28 U.S.C. § 1292(b) and Civil Local Rule 7.

INTRODUCTION

Defendants respectfully request that the Court certify for interlocutory appeal its July 28, 2025 order granting in part and denying in part Defendants' motions to dismiss. *See* ECF No. 148 ("Order"). Central to the Court's holding was the conclusion that a defendant's alleged continuous monitoring/exfiltration of data (including location data) from a device confers personal jurisdiction over that defendant wherever the plaintiff travels with that device. That important, contested, and purely legal question satisfies the requirements for certification under 28 U.S.C. § 1292(b).

First, there is substantial ground for difference of opinion over the jurisdictional question, which was highlighted but not resolved in the case on which this Court primarily relied, *Briskin v. Shopify, Inc.*, 135 F.4th 739 (9th Cir. 2025) (en banc). That decision addressed tracking software installed by the defendant (Shopify) around the time Shopify knew the plaintiff (Briskin) was in the forum. The Ninth Circuit acknowledged—but declined to address as "inapposite"—the dissent's concerns that a "traveling cookie" scenario (involving continuous monitoring) might give rise to jurisdiction wherever a plaintiff travels *after* the initial installation of tracking software.

But that is the exact scenario presented here. Plaintiff alleges that the tracking software was installed *outside* the forum, and that any exfiltration occurred in the United States because Defendants failed to *stop* tracking when Plaintiff traveled to the United States. As the *Briskin* dissent warned, finding jurisdiction in such a scenario flips the "express aiming" requirement of the purposeful direction test on its head, by letting a plaintiff's actions drive the jurisdictional analysis and having "jurisdiction attach[] if the company fails to 'expressly *avoid*' a forum." *Briskin*, 135 F.4th at 776 (Callahan, J., dissenting) (emphasis added). That is true whether or not the defendant knows about the subsequent travel (as would be the case in the dissent's "traveling cookie" scenario). Beyond that unanswered question from *Briskin*, both the First and Third Circuits have indicated that a defendant does not expressly aim conduct at a forum unless the defendant allegedly had contemporaneous knowledge of the device's location in the forum when the tracking began (as in *Briskin* but not here).

Second, the question is controlling and resolving it could materially advance the termination of this litigation. If resolved in Defendants' favor, the Court would lack personal jurisdiction and this case would be over. Indeed, resolving the question now is the most efficient path forward, given that discovery (and potentially a trial) could take years.

Third, certification is especially warranted in these circumstances. Defendants' due process injury—being subject to further proceedings before a court that lacks personal jurisdiction—cannot be cured by review after a final judgment at the end of those same proceedings. As *Briskin* demonstrates, this Court's reasoning implicates not only alleged hacking, but also online tracking software generally. The decision has ramifications for a wide range of litigation involving online retailers and other online platforms in the United States and worldwide—not to mention alleged

actions by foreign sovereigns (and U.S. allies). Because the question presented is exceptionally important and likely to recur, the Court should allow prompt resolution by the Ninth Circuit.

The Court should grant Defendants' motion to certify the Order under 28 U.S.C. § 1292(b).

BACKGROUND

In her original complaint, Plaintiff alleged that, in late 2015 or early 2016, the UAE government retained DarkMatter, a UAE company, to provide cybersecurity services. *See* ECF 1 ¶¶ 6, 67. Marc Baier, Ryan Adams, and Daniel Gericke, who had previously worked for a U.S. company that provided similar services to the UAE government, joined DarkMatter. *See id.* ¶ 69. Plaintiff alleged that, at some point before March 2018, DarkMatter hacked (from the UAE) her iPhone (located in the UAE) by sending an "iMessage." *See id.* ¶¶ 87-104. She alleged that the hack led to her arrest in the UAE, rendition to Saudi Arabia, and detention and torture there. *Id.* ¶¶ 117-118, 122-124. Plaintiff asserted claims against all Defendants for violating and conspiring to violate the Computer Fraud and Abuse Act, and an Alien Tort Statute claim against Baier, Adams, and Gericke. *Id.* ¶¶ 134-177.

On March 16, 2023, this Court dismissed Plaintiff's claims for lack of personal jurisdiction because Plaintiff's allegations failed all three mandatory steps of the due process inquiry. *See* ECF 44 at 20.

Plaintiff's Amended Complaint added new allegations. As most relevant here, Plaintiff alleges that, after she was hacked sometime "in 2017," she traveled to the United States "during th[e] period of surveillance." ECF 54 ¶¶ 134, 143. On Plaintiff's telling, Defendants "must have known that [Plaintiff] was in the United States," ECF 132 at 7, because Plaintiff's participation at a conference in the United States had been publicized on social media, ECF 54 ¶¶ 142-146. And because the device "continuously transmit[ted] data" during the alleged hack, Defendants

allegedly "exfiltrated … data from [her] device while she was physically present in the United States." *Id*. ¶¶ 24-28, 143-150. But Plaintiff alleges that Defendants exfiltrated data in the United States because they failed to *stop* tracking her here, not because they took any affirmative action within the forum. *E.g.,* ECF 132 at 16-17 ("Defendants *chose to leave their malware on her iPhone* and continue exfiltrating data from it even while knowing she was in the U.S.") (emphasis added); *id*. at 20 ("Although Defendants did not control Alhathloul's travel to the U.S., they *controlled their decision to continue exfiltrating her data* after they knew she traveled to the U.S.") (emphasis added).[1]

The Court granted in part and denied in part Defendants' motion to dismiss the Amended Complaint. In doing so, the Court held that it had personal jurisdiction over Defendants because Defendants purposefully directed their conduct at the United States. *See* Order 16-18; FED. R. CIV. P. 4(k)(2). The Court reasoned that, although Defendants allegedly installed malware on Plaintiff's phone when she and the device were outside the United States, Plaintiff "alleged intentional exfiltration of data from her iPhone while she was in the U.S.," and Plaintiff's allegations "support[ed] a strong inference at this stage that Defendants knew Plaintiff's location when they exfiltrated data from her device in the U.S." Order 17-18. The Court analogized those allegations to the allegations in *Briskin*, where the defendant "allegedly knew the location of consumers . . . either prior to or shortly after installing its initial tracking software onto their devices." *Id.* at 18 (quoting *Briskin*, 135 F.4th at 756). The Court distinguished *Walden v. Fiore*, 571 U.S. 277, 289 (2014)—in which the Supreme Court held that a plaintiff's contacts with the forum (even if

[1] For purposes of this motion, Defendants assume the truth of Plaintiff's allegations. *See* Order 9 (assessing whether "Plaintiff has alleged facts sufficient at this stage to make a prima facie showing of specific personal jurisdiction").

known by the defendant) cannot be attributed to the defendant for purposes of personal jurisdiction—on similar grounds. *See* Order 21.

ARGUMENT

The Court should state in writing that the dismissal order "involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the litigation[.]" 28 U.S.C. § 1292(b); *see Mohawk Indus. v. Carpenter*, 558 U.S. 110, 110-111 (2009). Reasonable jurists could disagree (and have disagreed) over the purely legal question of whether personal jurisdiction over a defendant who tracks a device is proper wherever that device travels, and deciding that question in Defendants' favor would end this case.

I. SUBSTANTIAL GROUNDS FOR DIFFERENCE OF OPINION EXIST AS TO WHETHER PERSONAL JURISDICTION OVER A DEFENDANT WHO TRACKS A DEVICE IS PROPER WHEREVER THE PLAINTIFF TRAVELS WITH THE DEVICE

Substantial grounds for difference of opinion exist over the critical jurisdictional question whether a defendant's alleged monitoring of data (including location data) from a device confers jurisdiction over that defendant wherever that device travels. Such "substantial grounds" exist when "fair-minded jurists might reach contradictory conclusions," such as when "the circuits are in dispute on the question and the court of appeals of the circuit has not spoken on the point" and/or "novel and difficult questions of first impression are presented." *ICTSI Oregon, Inc. v. Int'l Longshore & Warehouse Union*, 22 F.4th 1125, 1130 (9th Cir. 2022) (citations omitted). Further, "[t]he level of uncertainty required to find a substantial ground for difference of opinion should be adjusted to meet the importance of the question in the context of the specific case." 16 WRIGHT & MILLER'S FEDERAL PRACTICE & PROCEDURE § 3930 (3d ed.). "If proceedings that threaten to

endure for several years depend on an initial question of jurisdiction, . . . certification may be justified at a relatively low threshold of doubt." *Id.*

A. *Briskin* Expressly Left Open The Jurisdictional Question Presented By This Case

In denying Defendants' motion to dismiss, this Court held that, under the applicable "purposeful direction test," Plaintiff adequately alleged that Defendants expressly aimed intentional conduct at the United States. Order 13 (quoting *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 803 (9th Cir. 2004)). In doing so, the Court heavily relied on principles set forth in *Briskin,* which the Court found "broadened the circumstances in which a court may exercise specific personal jurisdiction over a defendant based on internet-related conduct, including the exfiltration of personal data." *Id.* at 9. To the Court, it was critical that Plaintiff alleged intentional exfiltration of data that occurred in the forum. *See id.* at 17-18.

The majority and dissent in *Briskin*, however, expressly left open the fact pattern presented here: whether jurisdiction is proper over a defendant not only in the place the defendant *installs* a cookie or other tracking software on a device, but everywhere the plaintiff chooses to subsequently travel during the period of exfiltration. In *Briskin*, the plaintiff alleged that the installation of tracking software occurred while the plaintiff was in the forum: "[W]hile knowing that the device Briskin was using to shop was located in California, Shopify surreptitiously implanted cookies that permanently remained on Briskin's device, tracked its physical location, and collected data[.]" 135 F.4th at 746; *see also id.* at 756 n.13 (Shopify knew Briskin's location before installing the cookie upon purchase because Shopify obtains location information when the consumer clicks on an item). The court held that the "target[ing] [of] California consumers" was not "mere happenstance" because "Shopify allegedly knew the location of consumers like Briskin either prior to or shortly after installing its initial tracking software onto their devices." *Id.* at 756. Shopify's

forum contacts were thus "its own choice and not random, isolated, or fortuitous." *Id.* at 758 (quotation omitted).

The *Briskin* dissent expressed concern that the majority's reasoning could "create[] a new 'traveling cookie' rule for *in personam* jurisdiction." 135 F.4th at 774 (Callahan, J., dissenting). Under that purported rule, when an alleged tortfeasor "attaches cookies [*i.e.*, tracking software] to a person's electronic device, jurisdiction attaches wherever that person happens to be, and indeed, *wherever that person happens to travel thereafter*." *Id.* (emphasis added). The dissent posited that if Shopify installed tracking software on Briskin's device while he was in California, but he then continued browsing in Nevada and Oregon, jurisdiction would attach in all three states. *See id.* In the dissent's view, that result would flout Supreme Court precedent by allowing the "'unilateral activity'" of the plaintiff "to drive the jurisdictional analysis." *Id.* at 776 (quoting *Kulko v. Superior Court of Cal.*, 436 U.S. 84, 93-94 (1978)).

On that question, reasonable minds could (and do) disagree on whether "express aiming" may include not only the *active* placement of tracking code on a device known to be located in the forum (as in *Briskin*), but also the *passive* tracking of the device as it is carried to a new forum (as in the traveling cookie hypothetical, and as alleged here). After all, in the former scenario, the defendants have sent something (the tracking code) to the forum. *See Walden*, 571 U.S. at 289. But in the latter scenario, the defendants have "never . . . sent anything" to the forum—the forum contact arguably results only from the *plaintiff's* unilateral decision to travel to the new forum (even if defendants have "knowledge of" that choice). *Id.* That key difference implicates *Walden*'s emphasis on "contacts that the defendant *himself* creates." *Id.* at 284 (citation omitted); *cf. Briskin*, 135 F.4th at 759 (unlike a defendant who never "'sent anything or anyone to [the forum],'" Shopify

"installs its software onto [consumers'] devices in California, and continues to track their activities") (quoting *Walden*, 571 U.S. at 289).

Crucially, the *Briskin* majority did not defend the expansive traveling cookie rule; instead, it merely rejected the dissent's concerns as "inapposite." 135 F.4th at 756 n.12; *see also* Order 20. That was because Shopify "allegedly committed its tortious activity *knowing Briskin's device was in California*"—unlike here, Briskin had not traveled to any other state during the relevant period. 135 F.4th at 756 n.12 (emphasis added). Moreover, the majority did "not look only to where Briskin was located at the time" the tracking software was installed, but also to additional ways Shopify targeted him and other California consumers. *See id.* at 755-756 & n.12 ("Shopify is alleged to target California consumers to extract, collect, maintain, distribute, and exploit for its own profit," both "California consumers' payment information" and "other personal identifying information."). Thus, the majority had no occasion to address whether jurisdiction would have been proper had the plaintiff traveled to California only *after* tracking software was installed; that "inapposite" question simply was not presented.

But it is presented here. As noted, Plaintiff does not allege that Defendants took affirmative action to install software or exfiltrate data from Plaintiff's device while she was in the United States. Instead, Plaintiff alleges only that Defendants failed to *stop* tracking an already-targeted device after she traveled to the forum. Plaintiff alleges a "continuous and ongoing hack" in which Plaintiff's device "continuously transmit[ted] data" to Defendants' servers. ECF 154 ¶¶ 127, 150; *see also* ECF 132 at 5 (Plaintiff arguing that malware "continuously transmit[ted] . . . data to Project Raven servers"); *id.* at 7 ("continuous surveillance"). And Plaintiff's brief opposing dismissal confirms that she is not alleging affirmative hacking in the United States, but rather that "Defendants *chose to leave their malware on her iPhone*." ECF 132 at 20 (emphasis added).

Accordingly, this case presents the very hypothetical that *Briskin* declined (and had no occasion) to resolve.

This Court appeared to agree that the "traveling cookie hypothetical" might pose serious jurisdictional problems, but distinguished that hypothetical based on Plaintiff's allegation that "Defendants retained control over whether data was exfiltrated to a DarkMatter-controlled server." Order 21. Respectfully, that allegation does not distinguish the *Briskin* dissent's scenario. Cookies, which are used by ecommerce retailers and others, pass "geolocation information" to the tracking entity. *Briskin*, 135 F.4th at 739.[2] In the traveling cookie hypothetical, the device owner continues browsing as he travels, such that the ecommerce retailer is aware of the user's location as he moves between different states. *See id.* at 774 (Callahan, J., dissenting) (user "keeps browsing" as he drives from California to Nevada, where he makes a purchase, then "visits another website" once in Oregon, all of which is tracked). In order not to track after a cookie is installed, companies may engage in "'geoblocking,' which restricts access to Internet content based on a user's geographic location," *id.* at 776 n.6, or otherwise take affirmative steps to disable the tracker. In other words, ecommerce entities that use tracking cookies (and thereby receive location information) "retain[] control over whether data" is collected, Order 21, in the same sense that Defendants were alleged to have "controlled their decision to continue exfiltrating [Plaintiff's] data" here, ECF 132 at 20. And the implications of finding jurisdiction in both scenarios is stark: "Now, instead of having to 'expressly aim' conduct at a forum, jurisdiction attaches if the company fails to 'expressly avoid' a forum." *Briskin*, 135 F.4th at 776 (Callahan, J., dissenting).

[2] *See also* CookieYes Blog, *A Guide To Tracking Cookies*, https://www.cookieyes.com/blog/tracking-cookies/ (last visited Aug. 15, 2025) ("Tracking cookies . . . collect data such as . . . location").

In short, this case presents the same question the *Briskin* majority declined to answer: whether jurisdiction over a defendant who installs tracking software on a plaintiff's device is proper "wherever that person happens to travel thereafter." *Briskin*, 135 F.4th at 774 (Callahan, J., dissenting). Indeed, under this Court's reasoning, personal jurisdiction would also be proper in the United States over a foreign ecommerce company (like Shopify) that installed a continuous-tracking cookie on a foreign plaintiff's foreign device during a foreign ecommerce transaction before she traveled to the United States on vacation. That important question is one the Ninth Circuit should have the opportunity to decide now.

B. Other Courts Have Contradicted This Court's Reasoning

"One of the best indications that there are substantial grounds for disagreement on a question of law is that other courts have, in fact, disagreed." *Brickman v. Facebook, Inc.*, No. 16-cv-00751, 2017 WL 1508719, at *3 (N.D. Cal. Apr. 27, 2017) (quoting *Heaton v. Social Fin., Inc.*, No. 14-cv-05191, 2016 WL 232433, at *4 (N.D. Cal. Jan. 20, 2016)). Beyond the disagreement between the *Briskin* majority and dissent over the implications of the majority's reasoning, the Third Circuit (relying on the First Circuit) has indicated that it would have reached a different conclusion than this Court. *See Hasson v. FullStory, Inc.*, 114 F.4th 181, 191 (3d Cir. 2024) (citing *Rosenthal v. Bloomingdales.com, LLC*, 101 F.4th 90, 98 (1st Cir. 2024)).[3]

In *Hasson*, the Third Circuit addressed allegations that pizza chain Papa Johns unlawfully "deployed" Session Replay Code (which "enables companies . . . to collect detailed information about the way visitors interact with [a] website") onto a customer's web browser while the

[3] The Third Circuit favorably cited the Ninth Circuit's (overruled) decision in *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201 (9th Cir. 2020), *overruled by Briskin*, 135 F.4th at 757. *See Hasson*, 114 F.4th at 190. Defendants do not rely on any part of the Third Circuit opinion resting on *AMA*'s discussion of differential targeting.

customer was in the forum state, Pennsylvania. 114 F.4th at 185, 188. The court "reject[ed] the argument that Papa Johns expressly targeted Pennsylvania simply because the data interception allegedly occurred in the forum." *Id.* at 191. The court was "not persuaded that transmitting computer code to a browser that happens to be in Pennsylvania is an intentional physical entry into the forum sufficient to establish express aiming[.]" *Id.* Rather, the plaintiff "had to allege that Papa Johns knew that a given user was in Pennsylvania *before* it sent the code to that user's browser." *Id*. The plaintiff "did not allege that Papa Johns knows that a given user is in Pennsylvania *before* the code is dispatched to his browser or that Papa Johns specifically sends the code *because* the user is located in Pennsylvania." *Id.* at 191-192.

As most relevant here, it did not matter "that Papa Johns' collection of users' geolocation data shows that the company inevitably knows it is capturing the website communications of Pennsylvania residents" once the tracking software is installed. *Hasson*, 114 F.4th at 192 (citation modified).[4] Instead, "a defendant's post hoc discovery that the tortious conduct was *received* in the forum, without more, does not establish that the company *targeted* (or expressly aimed its conduct at) the forum." *Id.* at 196 (quoting *IMO Indus., Inc. v. Kiekert AG*, 155 F.3d 254, 263 (3d Cir. 1998)) (emphasis added). The Third Circuit relied partly on a First Circuit decision holding that personal jurisdiction was lacking when a plaintiff failed to allege that the defendant "'*knew* that it was targeting the plaintiff in [the forum state]' at the time of the alleged wiretapping," rather than after the fact. *Id.* at 191 (quoting *Bloomingdales.com*, 101 F.4th at 97).

[4] Like tracking cookies, Session Replay Code can be disabled. *See* dynatrace, *Configure Session Replay for web applications*, https://docs.dynatrace.com/docs/observe/digital-experience/session-replay/configure-session-replay-web (last visited Aug. 15, 2025) (explaining how to configure Session Replay Code, including "enabling and disabling").

The Third and First Circuits thus approach the "express aiming" question by sensibly focusing on a defendant's knowledge at the time it deploys the cookie or other means of tracking. According to those cases' logic—which comports with *Briskin*'s emphasis on the company's alleged knowledge around the time it "install[ed] its *initial* tracking software," 135 F.4th at 756 (emphasis added))—a defendant aims its tortious conduct at the place where it sends the software. If a plaintiff subsequently travels to a new forum (and thus "*receive[s]*" tortious conduct there), the defendant does not (without more) "*target[]*" or "expressly aim[]" at the forum, even if it knows about that new location. *Hasson*, 114 F.4th at 196 (emphasis added). As indicated by this Court's decision to find personal jurisdiction in the latter scenario, reasonable jurists could disagree. At a minimum, the decisions of other courts amply show that the Order meets the "relatively low threshold of doubt" applicable to jurisdictional questions. 16 WRIGHT & MILLER, *supra*, § 3930.

II. THE JURISDICTIONAL QUESTION PRESENTED IS CONTROLLING, AND ITS RESOLUTION MAY MATERIALLY ADVANCE TERMINATION OF THE LITIGATION

The question is also controlling, and resolving it in Defendants' favor would end the U.S. litigation. "[A]ll that must be shown in order for a question to be 'controlling' is that resolution of the issue on appeal could materially affect the outcome of litigation in the district court." *In re Cement Antitrust Litig. (MDL No. 296)*, 673 F.2d 1020, 1026 (9th Cir. 1981). Indeed, "a question is controlling" in the relevant sense "if interlocutory reversal might save time for the district court, and time and expense for the litigants." 16 WRIGHT & MILLER, *supra*, § 3930. Any question that "involve[s] the possibility of avoiding trial proceedings, or at least curtailing and simplifying pretrial or trial," "may materially advance the ultimate termination of the litigation." *Id.*

The jurisdictional question presented easily satisfies that standard. If the Court lacks personal jurisdiction, "it will dispose of all further litigation." *Arthur v. Murphy Co.*, No. 10-cv-

3142, 2012 WL 13047758, at *3 (D. Or. Jan. 17, 2012). And if Defendants are correct that *Briskin* did not "broaden[] the circumstances in which a court may exercise specific personal jurisdiction" enough to reach Plaintiff's allegations, Order 9, the Court would lack personal jurisdiction over Defendants.

Certifying the Order is also the most efficient path forward. This case has been proceeding since December 2021. Discovery and (if necessary) a trial could potentially take years (and be exceedingly complex given Plaintiff's allegations implicating "UAE officials and the Saudi government," Order 32, among other issues). A decision from the Ninth Circuit could thus "conserve judicial resources, conserve party resources, and simplify case management." *Biederman v. FCA US LLC*, No. 23-cv-06640, 2025 WL 1266907, at *5 (N.D. Cal. May 1, 2025).

To be sure, the Order discussed additional purported contacts between Defendants and the United States. ECF 54 ¶ 108 (discussing, *e.g.*, Defendants' alleged use of "U.S.-based" technology to "mask[] the origin of their hacking transmissions"). But the Court focused primarily on the new allegation from Plaintiff's amended complaint that she had traveled to the United States in light of *Briskin*—with those other purported contacts merely providing "further support[]." Order 15, 24. Because the appeal could knock out the primary basis for jurisdiction, there is little question that an appeal "could materially affect the outcome of litigation in the district court." *In re Cement Antitrust Litig.*, 673 F.2d at 1026.

III. THE JURISDICTIONAL QUESTION IS EXCEPTIONALLY IMPORTANT AND RECURRING

Although finding the two prior prongs met is sufficient, certification is especially warranted here given the nature of Defendants' potential constitutional injuries and the Order's implications beyond this case.

"The advantages of immediate appeal increase with . . . the substantiality of the burdens imposed on the parties by a wrong ruling." 16 WRIGHT & MILLER, *supra*, § 3930. Along the same lines, section 1292(b) can "provide useful means of securing review of questions that elude effective review on appeal from final judgment." *Id.* Defendants' personal jurisdiction arguments rest on constitutional and statutory limitations on federal courts and Defendants' own asserted rights under the Due Process Clause—*i.e.*, their constitutional rights not to be subject to judicial proceedings in this forum. *See, e.g.*, *Shaffer v. Heitner*, 433 U.S. 186, 189 (1977). Because "[a] proceeding that has already happened cannot be undone," if Defendants are subject to discovery (and potentially trial) in violation of their due process rights, after-the-fact review of whether they could be subject to such proceedings "would come too late to be meaningful." *Cf. Axon Enter., Inc. v. FTC*, 598 U.S. 175, 191 (2023).

Additionally, although section 1292(b) does not require "a question [to] be important to a large number of other suits, . . . [t]he opportunity to achieve appellate resolution of an issue important to other cases may provide an additional reason for certification." 16 WRIGHT & MILLER, *supra*, § 3930. As this case, *Briskin*, and the out-of-circuit decisions involving alleged use of tracking software discussed above make clear, the jurisdictional question presented has potential to impact a broad range of internet-related litigation. An immediate appeal would thus provide clarity to courts, litigants, and businesses—including as to whether an out-of-forum defendant needs to take steps to "'expressly avoid' a forum" electronically to ensure that it will not be haled into court there. *Briskin*, 135 F.4th at 776 (Callahan, J., dissenting). Such clarity would promote a central purpose of the Due Process Clause: to "give[] a degree of predictability to the legal system that allows potential defendants to structure their primary conduct with some

minimum assurance as to where that conduct will and will not render them liable to suit." *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980).

Finally, Plaintiff's allegations implicate not only a foreign company, but also the UAE and Saudi Arabian governments. *See* Order 32. Those governments (which are both "key U.S. all[ies] in the Middle East," Order 54) have "procedural and substantive interests" against U.S. courts adjudicating such allegations. *Asahi Metal Indus. Co., Ltd. v. Super. Ct. of Cal.*, 480 U.S. 102, 115 (1987). But like Defendants' due process rights, those interests cannot be addressed adequately in an appeal *after* the adjudication takes place. And such adjudication would invite "other nations" to "hale our citizens into their courts" to adjudicate claims alleging unlawful surveillance by the U.S. government in the United States. *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124 (2013). The "[g]reat care and reserve [that] should be exercised when extending our notions of personal jurisdiction into the international field," *Asahi*, 480 U.S. at 114-115 (citation omitted), thus reinforces the need to ensure that jurisdiction is proper at the outset—and bolsters the case for certification here.

CONCLUSION

For the foregoing reasons, Defendants respectfully request that this Court state in writing that its Order granting in part and denying in part Defendants' motion to dismiss "involves a controlling question of law as to which there is substantial ground for difference of opinion and that an immediate appeal from the order may materially advance the ultimate termination of the litigation." 28 U.S.C. § 1292(b).

Respectfully submitted,

Dated: August 18, 2025

SCHWABE, WILLIAMSON & WYATT, P.C.

s/ Nika Aldrich
Nika Aldrich, OSB No. 160306
Telephone: (503) 222-9981

AKIN GUMP STRAUSS HAUER & FELD LLP

s/ Anthony T. Pierce
Anthony T. Pierce (*pro hac vice*)
James E. Tysse (*pro hac vice*)
jtysse@akingump.com
Caroline L. Wolverton (*pro hac vice)*
cwolverton@akingump.com
2001 K St., N.W.
Washington, D.C. 20006
Telephone: (202) 887-4000

ATTORNEYS FOR DEFENDANT DARKMATTER GROUP

SNELL & WILMER L.L.P.

s/ Clifford S. Davidson (by permission)
Clifford S. Davidson, OSB No. 125378
Telephone: (503) 624-6800

ATTORNEY FOR DEFENDANTS MARC BAIER, RYAN ADAMS, AND DANIEL GERICKE